AF

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant:	**Boris BALACHEFF et al.**	) Examiner:	Abdulhakim NOBAHAR
Serial No.:	**09/936,131**	) Art Unit:	2132
Filed:	September 4, 2001	) Our Ref:	B-4295PCT 619055-2 30001505-4US
For:	"SMARTCARD USER INTERFACE FOR TRUSTED COMPUTING PLATFORM"	) Date:	April 26, 2007
		) Re:	***Appeal to the Board of Appeals***

BRIEF ON APPEAL

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal from the Final rejection, dated December 1, 2006, for the above identified patent application. Please deduct the amount of $500.00 for the fee set forth in 37 C.F.R. 1.17(c) for submitting this Brief from deposit account no. 08-2025. Appellants submit that this Appeal Brief is being timely filed, since the Notice of Appeal was filed on March 1, 2007.

REAL PARTY IN INTEREST

The real party in interest to the present application is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC").HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA.The general or managing partner of HPDC is HPQ Holdings, LLC.

RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences related to the present application.

STATUS OF CLAIMS

Claims 1 – 38, 42, 43, 45, 46 and 48 - 61 are the subject of this Appeal and are reproduced in the accompanying appendix. Claims 39 – 41, 44 and 47 have been canceled.

STATUS OF AMENDMENTS

No Amendment After Final Rejection has been entered.

SUMMARY OF CLAIMED SUBJECT MATTER

The invention described and claimed in the present application relates generally to systems and methods for allowing a user of a computer to establish that the computer is trustworthy and that its operation has not been somehow corrupted (p. 3 ll. 22-29). The user is in possession of a token such as a smartcard which the user employs to verify that a computer is trustworthy (p. 3 ll. 30-35, p. 11 ll. 3-15). The computer or computing platform is equipped with a trusted component that is tamper-proof (p. 11 ll. 20-24) and that monitors the computing platform to ensure that its trustworthiness has not been subverted, such as by a virus (p. 12 ll. 1-15). The user's token requests the monitoring (trusted) component to provide certain data regarding the operating status of the computing platform and then compares that data with data resident on the token to determine whether the computing platform may be trusted by the user (p. 12 l. 32 – p. 13 l. 5) to engage in some sort of exchange such as a banking transaction (p. 13 ll. 6-11). If the token determines that the computing platform cannot be trusted, it can simply end communication/data exchange with the computing platform (p. 21 ll. 26-28) and/or deny required authorization for application programs running on the computing platform (p. 27, ll. 19-22). If the computing platform can be trusted, the token may cause the computing platform to display a verification message to the user to let the user know that the computing platform may be trusted (p. 28 ll. 15-20).

With greater particularity, the invention claimed in claim 1 is directed to a system of computing apparatus comprising a computing platform (10) having a first data processor (21)

and a first data storage means (p. 13 l. 35 – p. 15 l. 23); a monitoring component (24) having a second data processor (30) and a second data storage means (3), wherein said monitoring component is configured to perform a plurality of data checks on said computing platform (p. 15 l. 24 – p. 21 l. 31); and a token device (19) being physically distinct and separable from said computing platform and said monitoring component (p. 22 l. 8 – p. 23 l. 23), wherein in one mode of operation, said token device operates to make an integrity challenge to said monitoring component and said token device will not undertake specific actions of which it is capable unless it receives a satisfactory response to said integrity challenge (p. 23 l. 24 – p. 35 l. 9; Figs. 1- 12).

The invention claimed in claim 17 is directed to a system of computing apparatus comprising a computing platform (10) having a first data processor (21) and a first data storage means (p. 13 l. 35 – p. 15 l. 23); a monitoring component (24) having a second data processor (30) and a second data storage means (3), wherein said monitoring component is configured to perform a plurality of data checks on said computing platform (p. 15 l. 24 – p. 21 l. 31); and a token device (19) being physically distinct and separable from said computing platform and said monitoring component (p. 22 l. 8 – p. 23 l. 23), wherein said token device sends an integrity challenge to said monitoring component; said monitoring component generates a response to said integrity challenge; if said token device receives a satisfactory response to said integrity challenge, then said token device sends verification data to said computer platform, said verification data verifying correct operation of said computer platform; and said computer platform displays said verification data on a visual display screen (p. 23 l. 24 – p. 35 l. 9; Figs. 1-12).

The invention claimed in claim 18 is directed to a computing entity comprising a computing platform (10) having a first data processor (21) and first data storage means; a monitoring component (24) having a second data processor (30) and second data storage means (3), wherein said monitoring component is configured to perform a plurality of data checks on said computing platform, said monitoring component being capable of establishing an identity of itself (p. 15 l. 24 – p. 21 l. 31); interface means (12) for communicating with a token device (19), said interface means communicating with said monitoring component, wherein said computing entity is configured such that said monitoring component reports said data checks to said token

device, said data checks containing data describing a status of said computer platform (p. 23 l. 24 – p. 35 l. 9; Figs. 1- 12).

The invention claimed in claim 25 is directed to a method of obtaining verification of a state of a computer entity, said computer entity comprising a computer platform (10) comprising a first data processor (21) and a first memory means, and a monitoring component (24) comprising a second data processor (30) and a second memory means (3) (p. 15 l. 24 – p. 21 l. 31), said method comprising the steps of receiving an interrogation request signal via an interface (12) of said computing entity; said monitoring component performing a monitoring operation of said computer platform in response to a said received interrogation request signal; and said monitoring component reporting a result message to said interface, said result message describing a result of said monitoring operation (p. 23 l. 24 – p. 35 l. 9; Figs. 1- 12).

The invention claimed in claim 32 is directed to a method of obtaining verification of a state of a computer entity, said computer entity comprising a computer platform (10) and a monitoring component (24) (p. 15 l. 24 – p. 21 l. 31), said method comprising the steps of an application requesting access to a functionality from a token device (19); in response to said request for access to functionality said token device generating a request signal requesting a verification data from said monitoring component; in response to said request for verification, said monitoring component reporting a result message to said token device, said result message describing a result of a monitoring operation; by receipt of a satisfactory said result message, said token device offers said functionality to said application (p. 23 l. 24 – p. 35 l. 9; Figs. 1- 12).

The invention claimed in claim 38 is directed to a method of checking an integrity of operation of a computing entity, said computing entity comprising a computer platform (10) having a first processor means (21) and first data storage means, and a monitoring component (24) comprising a second processor (30) and second memory means (3) (p. 15 l. 24 – p. 21 l. 31), by means of a token device (19), said token device comprising a third data processor (61) and a third memory means (62) (p. 22 l. 8 – p. 23 l. 23), said method comprising the steps of programming said token device to respond to a received poll signal from an application program, said poll signal received from said computer platform; said token device receiving a poll signal from said computer platform; in response to said received poll signal, said token device generating a signal for requesting a verification operation by said monitoring component; and

said monitoring component performing a verification operation of said computer platform in response to said received signal from said token device (p. 23 l. 24 – p. 35 l. 9; Figs. 1- 12).

The invention claimed in claim 42 is directed to a method of verifying a status of a computing entity, by means of a token device (19) provided external of said computing entity, said method comprising the steps of said token device receiving a poll signal; said token device responding to said poll signal by providing a request for obtaining verification of a state of said computer entity; and said token device receiving a result message, said result message describing the result of said verification (p. 23 l. 24 – p. 35 l. 9; Figs. 1- 12).

The invention claimed in claim 43 is directed to a method by which a token device (19) can obtain verification of a state of a computing platform by using a monitoring component (24), said monitoring component being capable of performing at least one data check on said computer platform, and establishing an identity of itself, and establishing a report of said at least one data check (p. 15 l. 24 – p. 21 l. 31); and wherein said token device has data processing capability and behaves in an expected manner (p. 22 l. 8 – p. 23 l. 23); said token device being physically separable from said computing platform and said monitoring component, said token device having cryptographic data processing capability wherein, said monitoring component proves its identity to said token device and establishes a report to said token device of at least one data check performed on said computing platform (p. 23 l. 24 – p. 35 l. 9; Figs. 1- 12).

The invention claimed in claim 48 is directed to a computing system comprising a computing apparatus (10) having a first data processor (21) and a first memory; a monitoring component (24) having a second data processor (30) and a second memory (3), wherein said monitoring component is configured to perform a plurality of data checks on said computing apparatus (p. 15 l. 24 – p. 21 l. 31); and a portable user token (19) being physically distinct and separable from said computing apparatus and said monitoring component (p. 22 l. 8 – p. 23 l. 23), wherein in one mode of operation, said portable user token operates to make an integrity challenge to said monitoring component and said user computing device will not undertake specific actions of which it is capable unless a satisfactory response to said integrity challenge is provided (p. 23 l. 24 – p. 35 l. 9; Figs. 1- 12).

The invention claimed in claim 59 is directed to a computing entity comprising a computing platform (10) having a first data processor (21) and a first memory; a monitoring

component (24) having a second data processor (30) and a second memory (3), wherein said monitoring component is configured to perform a plurality of data checks on said computing platform (p. 15 l. 24 – p. 21 l. 31), a communications interface for communicating with a portable user token, said communications interface having a communication path to the monitoring component (p. 22 l. 8 – p. 23 l. 23), wherein said computing entity is configured such that said monitoring component is adapted to report said data checks to a portable user token connected to the communications interface, said data checks containing data describing a status of said computing platform (p. 23 l. 24 – p. 35 l. 9; Figs. 1- 12).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Issue 1: Whether Claims 1, 2, 10-26, 28-32, 38 and 41-61 are patentable under 35 U.S.C. 102(e) over U.S. Pat. No. 6,694,436 to Audebert (hereinafter "Audebert").

Issue 2: Whether Claims 3-9, 33, 34, 36 and 37 are patentable under 35 U.S.C. 103(a) over Audebert in view of U.S. Patent No. 6,230,266 to Perlman (hereinafter "Perlman").

ARGUMENT

Issue 1: Whether Claims 1, 2, 10-26, 28-32, 38 and 41-61 are patentable under 35 U.S.C. 102(e) over U.S. Pat. No. 6,694,436 to Audebert (hereinafter "Audebert").

In the final Action of December 1, 2006, the Examiner rejects claims 1, 2, 10-32, 38 and 41-61 under 35 U.S.C. 102(e) as being anticipated by U.S. Pat. No. 6,694,436 to Audebert. In particular, with regards to claims 1 and 48, the Examiner finds that Audebert discloses all claimed limitations. In their previous reply Appellants explained why they were compelled to respectfully disagree with the Examiner's interpretation and characterization of this document.

Specifically, Appellants explained that Audebert is directed to a computer system that includes a transaction terminal (1) able to communicate with a smart card (31). The transaction terminal includes a processor and memory, and is further able to communicate with another, physically discrete computer (server Sap or electronic unit) that runs a main software application (54/154) for conducting electronic transactions. The main application provides requests for information (signature, authentication, etc.) to the transaction terminal, where filter software F

(62) that is installed either on the terminal or on the smartcard operates to translate the high-level requests from the main application into elementary commands that can be executed by the smartcard. The filter software is also adapted to recognize whether the request is legitimate by verifying the identity of the main application from which the requests are received. It is important to note that the only method disclosed by Audebert for this type of verification is by the inclusion in the high-level requests of "information enabling the filter software F to verify its source and its integrity. Authentication can use a Message Authentication Code (MAC) or a code of the electronic signature type associated with the request. If the transaction is not entered by the user on the terminal module itself, the request can contain the information needed for the user to verify the essential data of the transaction, if required and if the terminal module supports this option." [col. 10 ll. 55-59] It is also of note that the filter software F is downloaded from the server Sap, and that the integrity of the filter software is also verified upon receipt: "To this end a message authentication code (MAC) can be associated with the downloaded program for verifying not only its integrity but also its source. The MAC can be generated using a symmetrical cryptography mechanism (DES in chained CBC mode). The source and integrity can also be verified using an asymmetrical cryptography mechanism: a condensate of the downloaded software is signed by the sender using their private key; the secure microprocessor 3 then verifies the signature using the sender's public key." [col. 23 l. 61 – col. 24 l. 3] Appellants noted that all such data verification and authentication by Audebert is thus based upon information contained within the transmitted data itself.

In the present Action, the Examiner continues to assert that "the electronic unit or the server Sap corresponds to the recited computing platform," "the terminal corresponds to the recited monitoring component" and that the smart card corresponds to the recited token device, and proceeds to find that Audebert discloses that said monitoring component is configured to perform a plurality of data checks on said computing platform by reasoning that "the terminal corresponds to the recited monitoring component which authenticates the application on the electronic unit or server and verifies the integrity of the data received from said application." As previously explained, Appellants respectfully submit that this interpretation of Audebert is incorrect because while the terminal of Audebert does indeed verify the integrity of data received from the server, this is **not** the same as performing data checks **on** the server. The terminal of

Audebert first receives data from the server and then, once the received data is in its possession, verifies its integrity – in other words, the terminal performs data integrity checks on the terminal, not on the server. This is not a mere matter of semantics; by performing data checks on the computing platform, the claimed invention assures the integrity of the platform itself, whereas the approach of Audebert can do no more than verify the integrity of the received data. Thus, as one illustrative example, the computing platform could be operating under the command of a rogue process that directs it to send data that would be verified as well as authenticated when received by the terminal of Audebert with no possibility of detecting the fact that the platform has been compromised. This is one type of scenario that the presently claimed invention seeks to subvert by providing a monitoring component that performs data checks on the computing platform.

On a more general level, Appellants previously also noted that Audebert is in effect concerned with the integrity of the terminal and with methods of preventing the downloading of malicious code onto, or acceptance of compromised data by, the terminal. Audebert does not in fact address at all the issue of server (computing platform) security. For this reason, Audebert teaches no more than verifying the identity of the server as it is coded into the transmitted data, and does not undertake any actions that can be understood as verifying the integrity of the server.

In the present Action, the Examiner replies to the above by asserting that "[t]he Examiner respectfully disagrees and asserts that Audebert discloses a system that the terminal unit (i.e. the monitoring component) authenticate the server (i.e., the computing platform) and *verifies the origin* of the request sent by the application installed on the electronic unit." Appellants do not understand why the Examiner thinks he disagrees with Appellants, because this is precisely Appellants' position and they agree wholeheartedly with the Examiner – namely, that Audebert teaches *verifying the origin of the request*. What the Examiner does not address anywhere in his reply is Appellants' further contention that verifying the origin of a request is not the same as performing data checks on the origin of the request (the computing platform). Appellants explained in great detail why this is so, and the Examiner wastes not one single word in his reply even acknowledging Appellants' discussion. Appellants thus beseech the Board to kindly consider all of the preceding, which can leave no doubt in the mind of the attentive reader that verifying the *origin* of data is not the same as verifying the *integrity of the origin* of data.

In view of the above, Appellants respectfully submit that claims 1 and 48 are in fact novel and allowable over Audebert and request the Board to overturn the Examiner on Appeal and pass these claims to issue.

Claims 2-16 and 45 depend from claim 1 and claims 49-58 depend from claim 48. In view of the above, Appellants submit that claims 2-16, 45 and 49-58 are also allowable at least based on their dependencies.

With respect to claims 17, 18 and 59, Appellants submit that the above discussion of claims 1 and 48 is equally probative of the novelty of these claims, and thus respectfully request that these claims be passed to issue as well.

Claims 19-24 and 46 depend from claim 18, and claims 60-61 depend from claim 59. Therefore, in light of the above discussion of claims 18 and 59, Applicants submit that claims 19-24, 46, and 60-61 are also allowable at least in view of their respective dependencies.

With respect to Appellants' previous discussion of the allowability of claim 25, the Examiner insists that Audebert discloses all claimed limitations including, *inter alia*, the claimed receiving an interrogation request signal via an interface of said computing entity and said monitoring component performing a monitoring operation of said computer platform in response to a said received interrogation request signal. Appellants have previously explained that there is in fact no interrogation request signal received by the server (computing platform) of Audebert; on the contrary, the requests in Audebert flow from the server to the terminal. There are no requests flowing from the terminal to the server because the terminal verifies the identity of the server solely based on the information contained in the requests received from the server. For this same reason, Audebert does not in fact disclose any actions that can be understood as performing a monitoring operation of the computing platform in response to a received interrogation request signal: namely, because (a) no such interrogation request signal is received by the computing platform, and (b) the only thing monitored by the terminal is the data received **from** the computing platform, not the computing platform itself.

In maintaining his rejection, "the examiner respectfully disagrees and asserts that Audebert discloses that the application installed on the electronic unit (i.e., the server) sends a request to the terminal unit related to a user transaction process (corresponding to the recited

receiving an interrogation request) and then the terminal unit authenticates the origin of the request (i.e. the server) (corresponding to the recited performing a monitoring operation)" and directs us to "see, for example, col. 6 lines 22-43, col. 7, lines 5-8, col. 9, lines 54-62 and col. 10, lines 7-14)."

Appellants respectfully submit that this statement borders on the illogical. What the Examiner is saying, very clearly, is that the terminal unit receives the request and then monitors itself. Appellants respectfully ask – even assuming, *arguendo*, that this is in fact what Audebert discloses, what does it have to do with Appellants' claimed monitoring component performing a monitoring operation of said computer platform in response to a said received interrogation request signal? If the terminal unit is the monitoring component (as the Examiner asserts on page 10 of the final Action), then what corresponds to the monitored computing entity? If the terminal unit receives the server request (as the Examiner asserts on page 3 of the final Action), then the Examiner is clearly asserting that the terminal unit corresponds to the claimed computing entity - in which case Appellants ask, what then corresponds to the monitoring component? With all due respect, Appellants submit that the Examiner's explanation is based on circuitous and self-contradictory logic that offers nothing on the face of Audebert that directly or even indirectly contradicts Appellants' contentions – namely that no interrogation request signal is received by the computing platform of Audebert, and that the only thing monitored by the terminal (that is, with respect to the first of the Examiner's two alternative interpretations of Audebert's terminal wherein it corresponds to the claimed monitoring component, not the claimed computing entity) is the *data received from* the computing platform, not the *computing platform itself.*

In view of the preceding, Appellants respectfully submit that claim 25 is also novel and allowable over Audebert and request the Board to overturn the Examiner on Appeal and pass this claim to issue as well.

Claims 26-31 depend from claim 25. Therefore, in light of the above discussion of claim 25, Appellants submit that claims 26-31 are also allowable at least in view of their dependency.

With regards to claim 32, Applicants make note of the previous discussion respecting claim 25, and in particular that there is no monitoring operation conducted by the terminal of Audebert, and thus there is no possibility of reporting a result message to said token device, said

result message describing a result of a monitoring operation, in the system of Audebert. Appellants therefore submit that claim 32 is allowable and respectfully request that the Board to kindly pass this claim to issue as well.

Claims 33-37 depend from claim 32. Therefore, in light of the above discussion of claim 32, Appellants submit that claims 33-37 are also allowable at least in view of their dependency.

With regards to claim 38, Appellants again refer to the above discussion and submit that Audebert does not disclose, at the very least, the claimed said monitoring component performing a verification operation of said computer platform in response to said received signal from said token device. As previously shown, Audebert does not teach nor allude to anything akin to performing a verification operation of the computer platform, but rather merely of information received from the computer platform. Appellants thus submit that claim 38 is allowable and respectfully request that the Examiner be overturned on Appeal and this claim be passed to issue.

With regards to claim 42, Appellants submit that the above discussion clearly proves that Audebert does not in fact disclose the claimed said token device responding to said poll signal by providing a request for obtaining verification of a state of said computer entity, and said token device receiving a result message describing the result of said verification, because there is no such verification being requested or conducted by or within the system of Audebert. Appellants thus submit that claim 42 is allowable and respectfully request the Board to pass this claim to issue.

With regards to claim 43, Appellants refer to the above discussion of claims 1 and 48 wherein it was shown that Audebert does not disclose the claimed monitoring component being capable of performing at least one data check on said computer platform. Appellants thus respectfully submit that claim 43 is not in fact anticipated and respectfully request the Board to also pass this claim to issue.

Issue 2: Whether Claims 3-9, 33, 34, 36 and 37 are patentable under 35 U.S.C. 103(a) over Audebert in view of U.S. Patent No. 6,230,266 to Perlman (hereinafter "Perlman").

Each of claims 3-5, 9, 33, 34, 36 and 37 has been addressed above by the discussion of their respective underlying independent claim, and Appellants thus submit that by virtue of these claims' dependencies, they are also allowable and are thus not

further individually addressed herein. Appellants therefore respectfully request that the rejection of these claims also be overturned on appeal and that these claims be passed to issue.

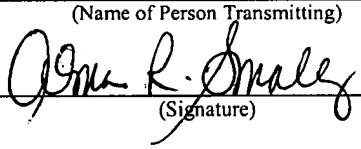
CONCLUSION

For the extensive reasons advanced above, Appellants respectfully contend that each pending claim is patentable. Therefore, reversal of all rejections and objections and re-opening of the prosecution is respectfully solicited.

I hereby certify that this correspondence is being deposited with the United States Post Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on

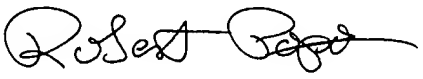
April 26, 2007
(Date of Transmission)

Alma Smalling
(Name of Person Transmitting)


(Signature)

4/26/07
(Date)

Respectfully submitted,



Robert Popa
Attorney for Applicants
Reg. No. 43,010
LADAS & PARRY
5670 Wilshire Boulevard, Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile
rpopa@ladasparry.com

Attachments

Claims

1. A system of computing apparatus comprising:

a computing platform having a first data processor and a first data storage means;

a monitoring component having a second data processor and a second data storage means, wherein said monitoring component is configured to perform a plurality of data checks on said computing platform; and

a token device being physically distinct and separable from said computing platform and said monitoring component,

wherein in one mode of operation, said token device operates to make an integrity challenge to said monitoring component and said token device will not undertake specific actions of which it is capable unless it receives a satisfactory response to said integrity challenge.

2. The system as claimed in claim 1, wherein said token device receives a detailed response to said integrity challenge, and processes said integrity response to interpret said integrity response.

3. The system as claimed in claim 1, further comprising a third party server, wherein a response to said integrity challenge is sent to said third party server.

4. The system as claimed in claim 3, wherein said monitoring component sends a detailed integrity response to a third party server if requested to do so in said integrity challenge.

5. The system as claimed in claim 3, wherein said monitoring component reports a detailed integrity response to said token device and said token device sends said integrity response to said third party server if it requires the third party server to help interpret said detailed integrity response.

6. The system as claimed in claim 3, in which a third party server simplifies said integrity response to a form in which said token device can interpret said integrity response.

7. The system as claimed in claim 6, wherein a third party server sends a simplified integrity

response to said token device.

8. The system as claimed in claim 7, operating to add a digital signature data to said simplified integrity response, said digital signature authenticating said third party server to said token device.

9. The system as claimed in claim 1, wherein said monitoring component sends a detailed integrity response to a third party server.

10. The system as claimed in claim 1, in which said token device is requested to take an action.

11. The system as claimed in claim 1 in which said token device requests to take an action.

12. The system as claimed in claim 1 in which said token device sends image data to said computer platform if a said satisfactory response to said integrity challenge is received, and said computer platform displays said image data.

13. The system as claimed in claim 1, wherein said monitoring component is capable of establishing an identity of itself.

14. The system as claimed in claim 1, further comprising an interface means for interfacing between said monitoring component and said token device.

15. The system as claimed in claim 1, wherein said system of computing apparatus is configured such that said monitoring component reports said data checks to said token device, said data checks containing data describing a status of said computer platform.

16. The system as claimed in claim 1, wherein a said specific action comprises authorising said computing platform to undertake a transaction on behalf of a user of said system.

17. A system of computing apparatus comprising:

a computing platform having a first data processor and a first data storage means;

a monitoring component having a second data processor and a second data storage means, wherein said monitoring component is configured to perform a plurality of data checks on said computing platform; and

a token device being physically distinct and separable from said computing platform and said monitoring component,

wherein said token device sends an integrity challenge to said monitoring component;

said monitoring component generates a response to said integrity challenge;

if said token device receives a satisfactory response to said integrity challenge, then said token device sends verification data to said computer platform, said verification data verifying correct operation of said computer platform; and

said computer platform displays said verification data on a visual display screen.

18. A computing entity comprising:

a computing platform having a first data processor and first data storage means;

a monitoring component having a second data processor and second data storage means, wherein said monitoring component is configured to perform a plurality of data checks on said computing platform, said monitoring component being capable of establishing an identity of itself;

interface means for communicating with a token device, said interface means communicating with said monitoring component,

wherein said computing entity is configured such that said monitoring component reports said data checks to said token device, said data checks containing data describing a status of said computer platform.

19. The computing entity as claimed in claim 18, wherein on communication between said token device and said interface means, said monitoring component is activated to perform a monitoring operation on said computer platform, in which said monitoring component obtains data describing an operating status of said computer platform.

20. The computing entity as claimed in claim 18, wherein said interface means is resident substantially wholly within said monitoring component.

21. The computing entity as claimed in claim 18, wherein said interface means is comprised by said computer platform.

22. The computing entity as claimed in claim 18, wherein said interface means comprises a PCSC stack in accordance with PCSC Workgroup PC/SC Specification 1.0.

23. The computing entity as claimed in claim 18, wherein said monitoring component comprises a verification means configured to obtain a certification data independently certifying said status data, and to provide said certification data to said interface means.

24. The computing entity as claimed in claim 18, wherein said interface means is configured to send and receive data according to a pro-active protocol.

25. A method of obtaining verification of a state of a computer entity, said computer entity comprising a computer platform comprising a first data processor and a first memory means, and a monitoring component comprising a second data processor and a second memory means, said method comprising the steps of:

receiving an interrogation request signal via an interface of said computing entity;

said monitoring component performing a monitoring operation of said computer platform in response to a said received interrogation request signal; and

said monitoring component reporting a result message to said interface, said result message describing a result of said monitoring operation.

26. A method as claimed in claim 25, in which said monitoring operation comprises the steps of:

said monitoring component carrying out one or a plurality of data checks on components of said computing platform; and

said monitoring component being able to report a set of certified reference data together with said data checks.

27. The method as claimed in claim 26, wherein said certified reference data includes a set of metrics to be expected when measuring particular components of said computing platform, and

includes digital signature data identifying an entity that certifies said reference data.

28. The method as claimed in claim 25, wherein said step of reporting verification of said monitoring operation comprises sending a confirmation signal to a token device said confirmation signal describing a result of said monitoring operation.

29. The method as claimed in claim 25, wherein said result message is transmitted by said interface to a token device external of said computing entity.

30. The method as claimed in claim 25, comprising the step of reporting a result of said monitoring operation by generating a visual display of confirmation data.

31. The method as claimed in claim 25, further comprising the step of adding a digital signature data to said result message, said digital signature data identifying said monitoring component; and

transmitting said result message and said digital signature data from said interface.

32. A method of obtaining verification of a state of a computer entity, said computer entity comprising a computer platform and a monitoring component, said method comprising the steps of:

an application requesting access to a functionality from a token device;

in response to said request for access to functionality said token device generating a request signal requesting a verification data from said monitoring component;

in response to said request for verification, said monitoring component reporting a result message to said token device, said result message describing a result of a monitoring operation;

by receipt of a satisfactory said result message, said token device offers said functionality to said application.

33. The method as claimed in claim 32, wherein said monitoring component sends a detailed integrity response to a third party server if requested in an integrity challenge by said token device.

34. The method as claimed in claim 32, wherein said monitoring component reports a detailed integrity response to said token device, and said token device sends said integrity response to a third

party server if it requires the third party server to help interpret said detailed integrity response.

35. The method as claimed in claim 34, wherein a third party server simplifies said integrity response to a form in which said token device can interpret said integrity response.

36. The method as claimed in claim 32, wherein a third party server sends a simplified integrity response to said token device.

37. The method as claimed in claim 32, further comprising the steps of:

adding a digital signature data to a simplified integrity response, said digital signature data authenticating a third party server to said token device.

38. A method of checking an integrity of operation of a computing entity, said computing entity comprising a computer platform having a first processor means and first data storage means, and a monitoring component comprising a second processor and second memory means, by means of a token device, said token device comprising a third data processor and a third memory means, said method comprising the steps of:

programming said token device to respond to a received poll signal from an application program, said poll signal received from said computer platform;

said token device receiving a poll signal from said computer platform;

in response to said received poll signal, said token device generating a signal for requesting a verification operation by said monitoring component; and

said monitoring component performing a verification operation of said computer platform in response to said received signal from said token device.

39. – 41. (canceled)

42. A method of verifying a status of a computing entity, by means of a token device provided external of said computing entity, said method comprising the steps of:

said token device receiving a poll signal;

said token device responding to said poll signal by providing a request for obtaining

verification of a state of said computer entity; and

said token device receiving a result message, said result message describing the result of said verification.

43. A method by which a token device can obtain verification of a state of a computing platform by using a monitoring component,

said monitoring component being capable of performing at least one data check on said computer platform, and establishing an identity of itself, and establishing a report of said at least one data check; and

wherein said token device has data processing capability and behaves in an expected manner;

said token device being physically separable from said computing platform and said monitoring component, said token device having cryptographic data processing capability

wherein, said monitoring component proves its identity to said token device and establishes a report to said token device of at least one data check performed on said computing platform.

44. (canceled)

45. A system as claimed in claim 1, wherein said token device is a smart card.

46. A system as claimed in claim 18, wherein said token device is a smart card.

47. (canceled)

48. A computing system comprising:

a computing apparatus having a first data processor and a first memory;

a monitoring component having a second data processor and a second memory, wherein said monitoring component is configured to perform a plurality of data checks on said computing apparatus; and

a portable user token being physically distinct and separable from said computing apparatus and said monitoring component,

wherein in one mode of operation, said portable user token operates to make an integrity

challenge to said monitoring component and said user computing device will not undertake specific actions of which it is capable unless a satisfactory response to said integrity challenge is provided.

49. The system as claimed in claim 48, wherein said portable user token receives a detailed response to said integrity challenge, and processes said integrity response to interpret said integrity response.

50. The system as claimed in claim 48, in which said portable user token is requested to take an action.

51. The system as claimed in claim 48 in which said portable user token requests to take an action.

52. The system as claimed in claim 48, wherein said monitoring component is capable of establishing an identity of itself.

53. The system as claimed in claim 48, further comprising token interface for interfacing between said monitoring component and said portable user token.

54. The system as claimed in claim 48, wherein said computing system is configured such that said monitoring component reports said data checks to said token device, said data checks containing data describing a status of said computer apparatus.

55. The system as claimed in claim 48, wherein the monitoring component is mounted on a common assembly with the first processor.

56. The system as claimed in claim 48, wherein one or more of said data checks comprise a check of the integrity of the basic input/output software for one or more components of the computing apparatus.

57. The system as claimed in claim 48, wherein the portable user token is a smart card.

58. The system as claimed in claim 53, wherein the portable user token is a smart card, and the token interface comprises a smart card reader.

59. A computing entity comprising:

a computing platform having a first data processor and a first memory;

a monitoring component having a second data processor and a second memory, wherein said monitoring component is configured to perform a plurality of data checks on said computing platform,

a communications interface for communicating with a portable user token, said communications interface having a communication path to the monitoring component,

wherein said computing entity is configured such that said monitoring component is adapted to report said data checks to a portable user token connected to the communications interface, said data checks containing data describing a status of said computing platform.

60. The computing entity as claimed in claim 59, wherein on communication between said portable user token and the communications interface, said monitoring component is activated to perform a monitoring operation on said computer platform, in which said monitoring component obtains data describing an operating status of said computer platform.

61. The computing entity as claimed in claim 59, wherein the communications interface is a smart card reader.

There is no evidence submitted with the present Brief on Appeal.

There are no other appeals or interferences related to the present application.